



Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-16

August 11, 2003

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at <http://www.nipc.gov>.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between July 17 and August 11, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified.

Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text. Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
121 Software ¹	Windows	121 WAM! 1.0.4	A Directory Traversal vulnerability exists in the 'CWD' command due to insufficient validation, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	121 WAM! Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Ambrosia Software, Inc. ²	Unix	Apple MacOS X 10.2-10.2.6, MacOS X Server 10.2-10.2.6	A vulnerability exists in the 'escapepod' screen saver software for Mac OS X, which could let a malicious user bypass password protection to obtain unauthorized access.	No workaround or patch available at time of publishing.	MacOS X Screen Effects Password Protection Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹ Secunia Security Advisory, August 7, 2003.

² SecurityFocus, July 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation ³ <i>More upgrades issued^{4, 5}</i>	Windows, MacOS X 10.x, Unix	Apache 2.0.43-2.0.46	A Denial of Service vulnerability exists due to an error in the type-map handler when parsing type maps.	Upgrade available at: http://httpd.apache.org/download.cgi <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/ <u>Mandrake:</u> http://www.mandrakesecure.net/en/ftp.php	Apache Web Server Type-Map Denial of Service	Low	Bug discussed in newsgroups and websites.
Apple ⁶ <i>Patch now available⁷</i>	Unix	MacOS X 10.2-10.2.6	A buffer overflow vulnerability exists in the screen saver password feature, which could let a malicious user cause obtain unauthorized access.	<i>Patch available at:</i> http://docs.info.apple.com/article.html?artnum=120232	MacOS X Screen Saver Password Buffer Overflow	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Atari800 Development ⁸	Unix	atari800 1.0.1-1.0.7, 1.2, 1.2.1 pre0, 1.2.1, 1.2.2	Multiple buffer overflow vulnerabilities exist due to insufficient bounds checking on user-supplied input before being copied into memory reserved buffers, which could let a malicious user obtain root access.	<u>Debian:</u> http://security.debian.org/pool/updates/contrib/a/atari800	Multiple Atari800 Emulator Buffer Overflows CVE Name: CAN-2003-0630	High	Bug discussed in newsgroups and websites.
BEA Systems, Inc. ⁹	Windows NT 4.0/2000, 2003, Unix	WebLogic Express 7.0 SP 3, Win32 7.0 SP 3, Weblogic Server 7.0 SP 3, Win32 7.0 SP 3	An access control vulnerability exists because certain code execution paths can be incorrect, which could let a remote malicious user impersonate a target user (including an administrative user) to gain their privileges.	Patches available at: ftp://ftpna.beasys.com/pub/releases/security/CR110892_700sp3.ja	WebLogic Server & WebLogic Express User Impersonation	Medium/High (High if root access can be obtained)	Bug discussed in newsgroups and websites.

³ SNS Advisory No.66, July 9, 2003.

⁴ Conectiva Linux Security Announcements, CLA-2003:698 & CLA-2003:704, July 21 & 24, 2003.

⁵ Mandrake Linux Security Update Advisory, MDKSA-2003:075, July 22, 2003.

⁶ Securiteam, July 6, 2003.

⁷ Securiteam, July 17, 2003.

⁸ Debian Security Advisory, DSA 359-1, July 31, 2003.

⁹ BEA Security Advisory, BEA03-35.00, July 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems, Inc. ¹⁰	Windows 95/98/ NT 4.0/2000, Unix	Liquid Data 1.1, WebLogic Express 5.1, SP1-SP13, 7.0, SP1-SP3, WebLogic Express for Win32 5.1, SP1-SP13, WebLogic Express for Win32 7.0, SP1-SP3, WebLogic Integration 2.1, 7.0, SP1, Weblogic Server 5.1, SP1-SP13, 7.0, SP1-SP3, WebLogic Server for Win32 5.1, SP1-SP13, 7.0, SP1-SP3	Multiple Cross-Site Scripting vulnerabilities exist in the console application and/or some of the samples provided by BEA because user-supplied HTML is not properly encoded, which could let a remote malicious user execute arbitrary HTML and script code.	Patches available at: ftp://ftpna.beasys.com/pub/releases/security/	WebLogic/ Liquid Data Multiple Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Bharat Mediratta ¹¹	Unix	Gallery 1.1-1.2.5, 1.3- 1.3.4	A Cross-Site Scripting vulnerability exists in the caption/description search feature due to insufficient verification of user-supplied input, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/gallery/gallery-1.3.4-pl1.tar.gz?download Debian: http://security.debian.org/pool/updates/main/g/gallery/	Gallery Search Engine Cross-Site Scripting CVE Name: CAN-2003-0614	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems ¹²	Multiple	IOS 12.0 (24.2)S, (24)S1, 12.2 (16.1)B, (16)B, (15.1)S, (15)ZN, (14.5)T, (14.5), (11)JA1	An information disclosure vulnerability exists when the Telnet service is enabled with authentication, which could let a remote malicious user obtain sensitive information.	Updates and workaround available at: http://www.cisco.com/warp/public/707/cisco-sn-20030724-ios-enum.shtml	Aironet Telnet Service Information Disclosure CVE Name: CAN-2003-0512	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁰ BEA Systems Security Advisory, BEA03-36.00, August 6, 2003.

¹¹ Debian Security Advisory, DSA 355-1, July 30, 2003.

¹² VIGILANTE Security Watch Advisory, July 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems ¹³	Multiple	IOS 8.2, 8.3, 9.0, 9.1, 9.14, R12.x, R11.x, 10.x, 11.x, 12.x	An information disclosure vulnerability exists in the echo service, which could let a remote malicious user obtain sensitive information.	<u>Workaround:</u> The vendor recommends disabling the udp-small-services using the following commands: no service udp-small-servers www.cisco.com/warp/public/707/cisco-sn-20030731-ios-udp-echo.shtml	IOS UDP Echo Service Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Cisco Systems ¹⁴	Multiple	IOS 12.2 (8)JA, 12.2 (4)JA1, 12.2 (4)JA, 12.2 (11)JA	A remote Denial of Service vulnerability exists when a malicious user submits a malformed HTTP GET request.	Updates and workaround available at: http://www.cisco.com/warp/public/707/cisco-sa-20030728-ap1x00.shtml	Cisco Aironet AP1x00 Malformed HTTP GET Denial of Service CVE Name: CAN-2003-0511	Low	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Cisco Systems ^{15, 16} <i>Cisco has updated advisory¹⁷</i>	Multiple	IOS 11.x, 12.x	A remote Denial of Service vulnerability exists when a malicious user submits a sequence of specifically crafted IPV4 packets.	Patches and workarounds available at: http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml <i>More software fixes now available at:</i> http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml	Cisco IOS Malicious IPV4 Packet Sequence Denial of Service CVE Name: CAN-2003-0567	High (High because IOS is a very widely deployed network operating system and vulnerability is currently being exploited in the wild)	Bug discussed in newsgroups and websites. Vulnerability can be exploited with utilities such as hping, so specific exploit code is not required to exploit this issue, however, exploit scripts have been published. Vulnerability has appeared in the press and other public media.

¹³ Cisco Security Notice, 44261, July 31, 2003.

¹⁴ VIGILANTE Security Watch Advisory, July 28, 2003.

¹⁵ Cisco Security Advisory, 44020 Rev. 1.9, July 22, 2003.

¹⁶ DHS/FedCIRC Advisory, FA-2003-15, July 17, 2003.

¹⁷ Cisco Security Advisory, 44020 Revision 1.13, August 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Colin Watson ¹⁸	Unix	man 2.3.18-2.3.20, 2.4, 2.4.1	Multiple buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in the 'add_to_dirlist()' function in the 'src/manp.c' file due to insufficient validation, which could let a malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'ult_src()' function in the 'src/ult_src.c' file due to an incorrect buffer size for the 'path' variable, which could let a malicious user execute arbitrary code; a buffer overflow vulnerability exists in '.So.' macros due to insufficient bounds checking, which could let a malicious user execute arbitrary code; and several buffer overflows exist in the processing of user-supplied 'PATH/MANPATH' values, which could let a malicious user execute arbitrary code.	Fixes available at: savannah.nongnu.org Debian: http://security.debian.org/pool/updates/main/m/man-db/	Multiple ManDB Utility Local Buffer Overflow CVE Name: CAN-2003-0620	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Colin Watson ¹⁹	Unix	man 2.3.18-2.3.20, 2.4, 2.4.1	A vulnerability exists because an arbitrary program can be specified as the location for a compressor utility, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	ManDB Compressor Binary Elevated Privileges	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Colin Watson ²⁰	Unix	man 2.3.20, 2.4.1	A vulnerability exists in the 'DEFINE' directive if man-db is installed to run as setuid, which could let a malicious user execute arbitrary code.	Debian: http://security.debian.org/pool/updates/main/m/man-db/	Man-db DEFINE Arbitrary Command Execution CVE Name: CAN-2003-0645	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Colin Watson ²¹	Unix	man 2.3.19	A buffer overflow vulnerability exists in the ManDB utility, which could let a malicious user execute arbitrary code.	Conectiva: ftp://ul.conectiva.com.br/updates/	ManDB Utility Buffer Overflow	High	Bug discussed in newsgroups and websites.

¹⁸ Debian Security Advisory, DSA 364-1, August 4, 2003.

¹⁹ Bugtraq, August 6, 2003.

²⁰ Debian Security Advisory, DSA 364-1, August 4, 2003.

²¹ SecurityFocus, July 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Constantin Kaplinsky ²²	Windows	TightVNC 1.2.0-1.2.7	A vulnerability exists in the handling of the 'QueryAllowNoPass' option when users authenticate, which could let a remote malicious user bypass authentication controls.	Upgrade available at: http://www.tightvnc.com/download.html	TightVNC 'QueryAllowNoPass' Authentication Bypass	Medium	Bug discussed in newsgroups and websites.
Counterpane ²³	Windows 2000, XP	Password Safe 1.92 b	A vulnerability exists because passwords and sensitive information can be recovered from memory even when the "Clear the clipboard when minimized" is enabled, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Password Safe Sensitive Information Recovery	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Debian ²⁴ <i>More updates available</i> 25, 26	Unix	Linux 3.0	A vulnerability exists because temporary files are created insecurely, which could let a malicious user overwrite arbitrary files.	Upgrade available at: http://security.debian.org/pool/updates/main/s/semi/ <i>RedHat:</i> ftp://updates.redhat.com/ <i>YellowDog:</i> ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/	SEMI/WEMI Insecure Temporary File Creation CVE Name: CAN-2003-0440	Medium	Bug discussed in newsgroups and websites.
D-Link ²⁷	Multiple	DI-704P	A remote Denial of Service vulnerability exists when a malicious user submits a request that is of excessive length.	No workaround or patch available at time of publishing.	DI-704P Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
e107.org ²⁸	Windows, Unix	e107 website system 0.554	A vulnerability exists in the 'class2.php' script due to insufficient filtering of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	e107 Website System HTML Injection	High	Bug discussed in newsgroups and websites. Exploits have been published.
EF Software ²⁹	Windows 95/98/NT/NT 4.0/2000, XP	EF Commander 3.54	A buffer overflow vulnerability exists in the routine used to parse FTP banners, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	EF Commander FTP Banner Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Every Buddy ³⁰	Windows, Unix	Every Buddy 0.4.3	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted instant message.	No workaround or patch available at time of publishing.	EveryBuddy Long Message Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

²² SecurityTracker Alert, 1007417, August 5, 2003.

²³ Bugtraq, August 3, 2003.

²⁴ Debian Security Advisory, DSA 339-1, July 6, 2003.

²⁵ Red Hat Security Advisory, RHSA-2003:234-01, July 23, 2003.

²⁶ Yellow Dog Linux Security Announcement, YDU-20030723-2, July 23, 2003.

²⁷ Bugtraq, August 6, 2003.

²⁸ Sec-Tec Advisory, July 25, 2003.

²⁹ Secunia Security Advisory, July 28, 2003.

³⁰ Securiteam, August 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Free RADIUS Server Project ³¹	Unix	Free RADIUS 0.5.0, 0.4.0, 0.3.0, 0.2.0, 0.8, 0.8.1	A buffer overflow vulnerability exists due to a boundary error in the code related to CHAP (Challenge-Handshake Authentication Protocol) authentication, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://ftp.freeradius.org/pub/radius/freeradius.tar.gz	FreeRadius Chap Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Freezing Cold Software ³²	Windows	aspBoard 1.2	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input for the URL variable, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	aspBoard Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
GameSpy Industries ³³	Windows	GameSpy Arcade	A vulnerability exists in 'GSAPAK.EXE' due to an input validation when handling '.APK' files, which could let a remote malicious user modify system information.	No workaround or patch available at time of publishing.	GameSpy Arcade GSAPAK.EXE	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
gURL Checker Project ³⁴	Unix	gURL Checker 0.6 .0-pre1&pre2	A remote Denial of Service vulnerability exists in 'html_parser.c' when a malicious user submits malformed HTML tags of excessive length.	Upgrade available at: http://www.nongnu.org/gurlchecker/#download	gURLChecker HTML Parser Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Hassan Consulting ³⁵	Unix	Shopping Cart 1.23	Several vulnerabilities exist: an information disclosure vulnerability exists in the configuration file, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the 'shop.cfg' file, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Shopping Cart Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser however, an exploit has been published.

³¹ SecurityTracker Alert, 1007325, July 29, 2003.

³² Zone-h Security Team Advisory, ZH2003-14SA, August 5, 2003.

³³ ThreeZee Technology, Inc. Security Advisory, TZT002, July 31, 2003.

³⁴ SecurityFocus, August 5, 2003.

³⁵ Indonesia Security Development Team Advisory, July 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company ³⁶	Multiple	LaserJet 4550	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the default configuration due to insufficient filtering of HTML input, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because the device is set without a password by default, which could let a remote malicious user obtain unauthorized access to the web-based administration interface	No workaround or patch available at time of publishing.	LaserJet 4550 Cross-Site Scripting & Default Password	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard Company ³⁷	Unix	PHNE_26413, PHNE_27128	A Denial of Service vulnerability was introduced in the PHNE_27128 and PHNE_26413 patches.	The vendor has reported that because this patch does not contain critical fixes it should be removed, details regarding patch removal can be found in the referenced advisory at: ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/	HP PHNE_26413 & PHNE_27128 Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Company ³⁸	Windows	Compaq Insight Management Agents 5.0 H	A format string vulnerability exists in the processing of 'DebugSearchPaths' HTTP requests, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Compaq Insight Management Agent Format String	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Hewlett Packard Company ³⁹	Unix	HP-UX 11.0, 11.11, 11.22	A remote Denial of Service vulnerability exists when handling some types of network traffic.	Patches available at: http://itrc.hp.com	HP-UX Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Hideki Kimata ⁴⁰	Unix	xtok-kaetama 1.0 b-6	A buffer overflow vulnerability exists in the '-nickname' command line option due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Xtokkaetama Nickname Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Hideki Kimata ⁴¹	Unix	xtok kaetama 1.0 b-6	Two buffer overflow vulnerabilities exist when processing the display command line option and the 'XTOKKAETAMADIR' environment variable, which could let a malicious user execute arbitrary code.	Patches available at: http://security.debian.org/pool/updates/main/x/xtokkaetama/	Xtokkaetama Buffer Overflow CVE Name: CAN-2003-0611	High	Bug discussed in newsgroups and websites.

³⁶ Exploitlabs.com Advisory, EXPL-A-2003-018, July 24, 2003.

³⁷ Hewlett-Packard Company Security Bulletin, HPSBUX0307-270 Rev. 01, July 29, 2003.

³⁸ Secunia Security Advisory, August 6, 2003.

³⁹ Hewlett-Packard Company Security Bulletin, HPSBUX0307-271, July 29, 2003.

⁴⁰ Bugtraq, August 3, 2003.

⁴¹ Debian Security Advisory, DSA 356-1, July 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hughes Billing ⁴²	Multiple	Hughes Billing	An information disclosure vulnerability exists in the 'config' and 'htpasswd' files, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Hughes Billing Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hughes Technologies ⁴³	Unix	Mini SQL (mSQL) 1.0, 1.3	A vulnerability exists due to a format string error in the 'mysqlSelectDB' query function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Mini SQL Remote Format String	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Hugo Rabson ⁴⁴	Unix	Mindi 0.58 r5	A vulnerability exists due to insecure creation of temporary files, which could let a malicious user obtain elevated privileges.	Debian: http://security.debian.org/pool/updates/main/m/mindi/	mind Temporary File Creation CVE Name: CAN-2003-0617	Medium	Bug discussed in newsgroups and websites.
IBM ⁴⁵	Unix	DB2 Universal Database for AIX 6.0, 6.1, 7.0-7.2, Universal Database for HP-UX 6.0, 6.1, 7.0-7.2, Universal Database for Linux 6.0, 6.1, 7.0-7.2, Universal Database for Solaris 6.0, 6.1, 7.0-7.2	A vulnerability exists because members of group 'db2asgrp' can use the setuid root 'db2job' binary to write arbitrary files, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	DB2 'db2job' Arbitrary File Overwrite	High	Bug discussed in newsgroups and websites. Exploit has been published.

⁴² Securiteam, July 31, 2003.

⁴³ Securiteam, July 28, 2003.

⁴⁴ Debian Security Advisory, DSA 362-1, August 2, 2003.

⁴⁵ Bugtraq, August 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM ⁴⁶	Unix	DB2 Universal Database for AIX 6.0, 6.1, 7.0-7.2, 8.0, 8.1, Universal Database for HP-UX 6.0, 6.1, 7.0-7.2, 8.0, 8.1, Universal Database for Linux 6.0, 6.1, 7.0-7.2, 8.0, 8.1, Universal Database for Solaris 6.0, 6.1, 7.0-7.2, 8.0, 8.1	A vulnerability exists because a number of shared libraries are stored in a directory owned by the user and group 'bin' and setuid root utilities are linked to these libraries, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	DB2 Shared Library Root Access	High	Bug discussed in newsgroups and websites. Exploit has been published.
Invision Power Services ⁴⁷	Windows, Unix	Invision Board 1.0, 1.0.1, 1.1.1, 1.1.2, 1.2	An input validation vulnerability exists because overlapping IBF tags are not processed properly, which could let a remote malicious user submit a specially crafted message that will modify the appearance of the web page.	No workaround or patch available at time of publishing.	Invision Board Overlapping IBF Formatting Tag	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
J. Schilling ⁴⁸	Unix	CDRTools 2.0, 2.0.3	A vulnerability exists in the 'rscsi' binary, which could let a malicious user obtain root privileges.	Upgrade available at: http://freshmeat.net/releases/131136/	CDRTools RSCSI Debug File Arbitrary Local File Manipulation	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
KodeIT ⁴⁹	Windows	IISShield 1.0, 1.0.1	A vulnerability exists because certain malicious malformed requests are not dropped, which could let a remote malicious user submit a packet will bypass security.	Upgrade available at: http://www.kodeit.org/tools/iisshield.zip	IISShield Unspecified Scan Bypass	Medium	Bug discussed in newsgroups and websites.
Macro-media ⁵⁰	Windows, MacOS X, Unix	Dreamweaver MX 6.0	A Cross-Site Scripting vulnerability exists because the 'accessdenied' parameter isn't properly verified before it is returned to the user, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Dreamweaver MX Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁴⁶ Bugtraq, August 5, 2003.

⁴⁷ SecurityTracker Alert, 1007405, August 4, 2003.

⁴⁸ Secure Network Operations, Inc. Advisory, SRT2003-08-01-0126, August 1, 2003.

⁴⁹ Secunia Security Advisory, August 5, 2003.

⁵⁰ SecurityTracker Alert ID, 1007399, August 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Martin Preishuber ⁵¹	Unix	eroaster 2.0	A vulnerability exists due to insufficient security precautions when creating a temporary file for use as a lockfile, which could let a malicious user obtain elevated privileges.	<u>Debian:</u> http://security.debian.org/pool/updates/main/e/eroaster/	ERoaster Insecure Temporary File Creation CVE Name: CAN-2003-0656	Medium	Bug discussed in newsgroups and websites.
Microsoft ⁵² <i>Microsoft updates bulletin</i> ⁵³	Windows NT	Windows NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6	A remote Denial of Service vulnerability exists in the 'GetCanonicalPath()' function because memory that the function does not own can be freed when a specially crafted request is submitted, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code. <i>Bulletin was updated to provide details of problem when patch is installed on systems running RRAS Service.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-029.asp	Windows NT File Management Function Remote Denial of Service CVE Name: CAN-2003-0525	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft ⁵⁴	Windows 95/98/SE/ NT 4.0	Outlook Express 5.0, 5.01, 5.5, 6.0	A recurrence of a previously fixed vulnerability exists because a remote malicious user can embed HTML with active scripting code in a plain text e-mail message and send it to a Microsoft Outlook Express (OE) user.	No workaround or patch available at time of publishing.	Outlook Express Script Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁵¹ Debian Security Advisory, DSA 366-1, August 6, 2003.

⁵² Microsoft Security Bulletin, 03-029, July 23, 2003.

⁵³ Microsoft Security Bulletin, 03-029 V1.1, July 29, 2003.

⁵⁴ NTBugtraq, July 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ^{55, 56} <i>Multiple exploits have been published and several Trojans circulating.⁵⁷</i> <i>Mblast worm circulating in the wild.</i>	Windows 98/NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, Server 2003 Standard Edition, Server 2003 Web Edition, Windows XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability exists in the RPC interface that implements the Distributed Component Object Model services (DCOM) due to insufficient bounds checking of client DCOM object activation requests, which could let a malicious user install programs, view, change or delete data, create new accounts with full privileges or execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp	Windows DCOM RPC Buffer Overflow CVE Name: CAN-2003-0352	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media. <i>Multiple exploit scripts have been published. There is currently at least one autorooter-enabled IRC bot circulating that exploits this vulnerability. Also multiple Trojans are circulating that exploit the vulnerability.</i>

⁵⁵ Microsoft Security Bulletin, MS03-026 V1.2, July 21, 2003.

⁵⁶ Department of Homeland Security Advisory, July 24, 2003.

⁵⁷ SecurityFocus, August 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
mnoGo Search ⁵⁸ <i>Conectiva issues upgrade</i> ⁵⁹	Windows, Unix	mnoGo Search 3.2.10, 3.1.20	Two buffer overflow vulnerabilities exist due to boundary errors when handling user input supplied to the 'ul' and 'tmplt' parameters, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.mnogosearch.org/download.html <i>Conectiva:</i> ftp://atualizacoes.conectiva.com.br/	MNOGo Search 'ul' & 'tmplt' Parameters Buffer Overflows	High	Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.
Multiple Vendors ⁶⁰	Unix	Linux kernel 2.4.20	A remote Denial of Service vulnerability exists in kernels built supporting the 'CONFIG_IP_NF_CONNTR ACK' option or with the 'IP_conntrack' module loaded.	Patch available at: http://downloads.securityfocus.com/vulnerabilities/patches/netfilter-ipconntrack.patch	Netfilter Connection Tracking Remote Denial of Service CVE Name: CAN-2003-0187	Low	Bug discussed in newsgroups and websites.
Multiple Vendors ⁶¹	Unix	Linux kernel 2.4.20, 2.4.21, pre7, pre4, pre1	A remote Denial of Service vulnerability exists due to an error when the system performs NAT (Network Address Translation) if the modules 'ip_nat_ftp' or 'ip_nat_irc' are loaded, or 'CONFIG_IP_NF_NAT_FTP' or 'CONFIG_IP_NF_NAT_IRC' is enabled.	Patch available at: http://downloads.securityfocus.com/vulnerabilities/patches/netfilter-ircftp-nat.patch	Netfilter NAT Remote Denial of Service CVE Name: CAN-2003-0467	Low	Bug discussed in newsgroups and websites.
Multiple Vendors ⁶²	Unix	Linux kernel 2.4.0-test1-2.4.0-test12, 2.4-2.4.17, 2.4.18, 2.4.18 x86, 2.4.18 pre-1-2.4.18 pre-8, 2.4.19, 2.4.19 - pre1-2.4.19 pre6, 2.4.20, 2.4.21, 2.4.21 pre1, 2.4.21 pre4	A remote Denial of Service vulnerability exists in the 'decode_fh' function in 'nfs3xdr.c' due to a failure to handle a negative size value in certain NFS calls.	No workaround or patch available at time of publishing.	Linux Kernel 2.4 'nfsexdr.c' Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

⁵⁸ Securiteam, June 11, 2003.

⁵⁹ Conectiva Linux Security Announcement, CLA-2003:711, July 28, 2003.

⁶⁰ Netfilter Core Team Security Advisory, August 2, 2003.

⁶¹ Netfilter Core Team Security Advisory, August 2, 2003.

⁶² Bugtraq, July 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 63, 64, 65 <i>More advisories issued</i> ^{66, 67} <i>Conectiva issues upgrade</i> ⁶⁸	Unix	Linux kernel 2.4.0-test1-test12, 2.4-2.4.20, 2.4.21 pre1&pre4	A vulnerability exists in the MXCSR handler code due to a failure to handle malformed address data.	<u>Debian:</u> http://security.debian.org/pool/updates/main/k/ <u>Mandrake:</u> ftp://ftp.planetmirror.com/pub/Mandrake/updates/9.1/RPMS/ <u>RedHat:</u> ftp://updates.redhat.com/ <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/	Linux Kernel MXCSR Handler Malformed Address CVE Name: CAN-2003-0248	Low	Bug discussed in newsgroups and websites.
Multiple Vendors ⁶⁹	Multiple	Compaq 686T2 v08.22.1999; Dell Latitude CPx H* revision A09, CPi A* revision A15; IBM ThinkPad X IZET9AW W 2.22; Phoenix Technologies BIOS R0217U0; SystemSoft BIOS R1.04; Toshiba Satellite 1410-303 1.20	A Denial of Service vulnerability exists due to improper implementation of newly (from Pentium II and above) introduced system calls (SYSENTER/SYSEXIT).	No workaround or patch available at time of publishing.	Multiple Vendor BIOS SYSENTER Denial of Service	Low	Bug discussed in newsgroups and websites.

⁶³ Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.

⁶⁴ Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.

⁶⁵ Mandrake Linux Security Update Advisory, MDKSA-2003:066, June 11, 2003.

⁶⁶ Red Hat Security Advisory, RHSA-2003:195-06, June 19, 2003.

⁶⁷ Debian Security Advisory DSA 332-1 & 336-1, June 27 & 29, 2003.

⁶⁸ Conectiva Linux Security Announcement, CLA-2003:701, July 22, 2003.

⁶⁹ Securiteam, July 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁷⁰ <i>Exploit script published and more upgrades issued</i> ^{71, 72, 73}	Unix	Linux kernel 2.4.0-test1-2.4.0-test12, 2.4.17, 2.4.18, 2.4.18 x86, 2.4.18 pre-1-2.4.18 pre-8, 2.4.19, 2.4.19 - pre1-2.4.19 - pre6, 2.4.20, 2.4.21, 2.4.21 pre1, 2.4.21 pre4	Multiple vulnerabilities exist: an information disclosure vulnerability exists due to a flaw in '/proc/tty/driver/serial,' which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists due to a race condition in the execve() system call; an access control vulnerability exists because a malicious user can bind services to UDP ports that have already been allocated; an access control vulnerability exists in the 'execve()' because the file descriptor of an executable process is recorded in the calling process's file table, which could let a malicious user obtain sensitive information; a vulnerability exists in the '/proc' filesystem, which could let a malicious user obtain sensitive information; a remote Denial of Service vulnerability exists in the Spanning Tree Protocol (STP) implementation due to insufficient validation of user-supplied input; a vulnerability exists because the bridge topology can be modified due to the inherent insecurity of the STP protocol, which could let a remote malicious user modify information; and a vulnerability exists in the forwarding table, which could let a remote malicious user spoof packets.	Engarde: http://infocenter.guardian.digital.com/advisories/ RedHat: ftp://updates.redhat.com/ Conectiva: ftp://ul.conectiva.com.br/updates/ Debian: http://security.debian.org/pool/updates/main/k/ Mandrake: http://www.mandrakesecurity.net/en/advisories/	Multiple Linux 2.4 Kernel Vulnerabilities CVE Names: CAN-2003-0461, CAN-2003-0462, CAN-2003-0464, CAN-2003-0476, CAN-2003-0501, CAN-2003-0550, CAN-2003-0551, CAN-2003-0552	Low/Medium (Medium if sensitive information can be obtained or elevated privileges are obtained)	Bug discussed in newsgroups and websites. <i>Proof of Concept exploit has been published for the execve() system call Denial of Service.</i>
Multiple Vendors ⁷⁴ <i>Engarde issues patch</i> ⁷⁵	Unix	Linux kernel 2.2-2.2.25, 2.4.1-2.4.21	An information disclosure vulnerability exists in the /proc filesystem when setuid applications are invoked, which could let a malicious user obtain sensitive information.	Engarde: http://infocenter.guardian.digital.com/advisories/	Linux /proc Filesystem Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

⁷⁰ Red Hat Security Advisory, RHSA-2003:238-01, July 21, 2003.

⁷¹ Mandrake Linux Security Update Advisory, MDKSA-2003:074, July 15, 2003.

⁷² Conectiva Linux Announcement, CLSA-2003:712, July 28, 2003.

⁷³ Debian Security Advisories, DSA 358-21 & DSA 358-2, July 31, 2003 & August 5, 2003.

⁷⁴ Bugtraq, June 20, 2003.

⁷⁵ Guardian Digital Security Advisory, ESA-20032407-018, July 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 76, 77, 78, 79, 80, 81, ,82, 83	Unix	FreeBSD 4.0, alpha, 4.0.x, 4.1, 4.1.1, Stable, Release, 4.2, Release, Stable, Stablepre05 0201, pre122300, 4.3, Release, Releng, Stable, 4.4, Releng, Stable, 4.5, Release, Stable, 4.5 Stablepre20 02-03-07, 4.6, Release, Stable, 4.6.2, 4.7, Release, Stable, 4.8, PreRelease, 5.0, alpha; NetBSD 1.5-1.5.3, 1.6, 1.6.1; OpenBSD 2.0-2.9, 3.0-3.3; RedHat wu-ftp- 2.6.1- 16.i386. rpm, 16.ppc. rpm, 18.i386. rpm, 18.ia64. rpm, -2.6.2- 5.i386. rpm, 8.i386.rpm; Washing- ton University wu-ftp 2.5.0, 2.6.0-2.6.3	A buffer overflow vulnerability exists due to an off-by-one error in the 'fb_realpath()' function when calculating the length of a concatenated string, which could let a remote malicious user obtain root privileges.	Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/w/wu-ftp/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:08/realpath.patch Mandrake: http://www.mandrakesecure.net/en/ftp.php NetBSD: ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2003-011-realpath.patch OpenBSD: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/ RedHat: ftp://updates.redhat.com/ SuSE: ftp://ftp.suse.com/pub/suse/	Multiple Vendor realpath() Off-By-One Buffer Overflow CVE Name: CAN-2003-0466	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.

⁷⁶ Debian Security Advisory, 357-1, July 31, 2003.

⁷⁷ Mandrake Linux Security Update Advisory, MDKSA-2003:080, July 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 84, 85, 86 <i>More advisories issued</i> ⁸⁷ <i>Conectiva issues upgrade</i> ⁸⁸	Unix	Linux kernel 2.0-2.0.39, 2.1, 2.1.89, 2.2-2.2.25, 2.3, 2.3.99, 2.3.99 pre1-pre7, 2.3.99, 2.4.0-test1-test12, 2.4-2.4.21 pre4, 2.5.0-2.5.69; RedHat Linux 7.1, i386, i586, i686, 7.2, athlon, i386, i586, i686, 7.3, i386, i686, 8.0, i386, i686, 9.0 i386	A Denial of Service vulnerability exists in the TTY layer.	<u>Debian:</u> http://security.debian.org/pool/updates/main/k/ <u>Mandrake:</u> ftp://ftp.planetmirror.com/pub/Mandrake/updates/9.1/RPMS/ <u>RedHat:</u> ftp://updates.redhat.com/ <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/	Linux TTY Layer Denial of Service CVE Name: CAN-2003-0247	Low	Bug discussed in newsgroups and websites.

⁷⁸ Red Hat Security Advisory, RHSA-2003:245-01, July 31, 2003.

⁷⁹ SuSE Security Announcement, SuSE-SA:2003:032, July 31, 2003.

⁸⁰ Conectiva Linux Security Announcement, CLA-2003:715, August 1, 2003.

⁸¹ FreeBSD Security Advisory, FreeBSD-SA-03:08, August 4, 2003.

⁸² NetBSD Security Advisory 2003-01, August 4, 2003.

⁸³ Turbolinux Security Advisory, TLSA-2003-46, August 4, 2003.

⁸⁴ Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.

⁸⁵ Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.

⁸⁶ Mandrake Linux Security Update Advisory, MDKSA-2003:066, June 11, 2003.

⁸⁷ Debian Security Advisories, DSA 332-1 & 336-1, June 27 & 29, 2003.

⁸⁸ Conectiva Linux Security Announcement, CLA-2003:701, July 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{89, 90, 91, 92, 93,}	Unix	KDE Konqueror 2.1.1, 2.2.2, 3.0-3.0.3, 3.0.5, 3.1, 3.1.1, Konqueror Embedded 0.1	A vulnerability exists in the 'user:password@host' form because authentication credentials are not removed from URLs in the HTTP-Referrer header, which could let a remote malicious user obtain sensitive information.	KDE: http://ftp.kde.org/pub/kde/security_patches Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2003-236.html Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/kde/*.tgz ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/kdei/*.tgz	Konqueror HTTP REFERER Authentication Disclosure CVE Name: CAN-2003-0459	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
NetBSD ⁹⁴	Unix	NetBSD 1.5-1.5.3, 1.6, 1.6.1	A remote Denial of Service vulnerability exists in systems that have OSI networking support compiled into their kernel because error-reporting functions are not implemented correctly.	Details on upgrades available at: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-010.txt.asc	NetBSD Kernel OSI Remote Denial of Service CVE Name: CAN-2003-0653	Low	Bug discussed in newsgroups and websites.
NetScreen ⁹⁵	Windows 2000	ScreenOS 4.0.1 r1-4.0.1 r6, 4.0.3 r1&r2	A remote Denial of Service vulnerability exists when a malicious user modifies the system configuration values that control the TCP windows size.	Upgrades and workaround available at: http://www.netscreen.com/services/security/alerts/advisory-57739.txt	ScreenOS Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁸⁹ Turbolinux Security Advisory, TLSA-2003-45, July 30, 2003.

⁹⁰ RedHat Security Advisories, RHSA-2003:236-08 & RHSA-2003:235-01, July 30, & August 11, 2003.

⁹¹ Mandrake Linux Security Update Advisory, MDKSA-2003:079, July 31, 2003.

⁹² Debian Security Advisories, DSA 361-1 & DSA 361-2, August 1 & 11, 2003.

⁹³ Slackware Security Advisory, SSA:2003-213-01, August 3, 2003.

⁹⁴ NetBSD Security Advisory, 2003-010, August 4, 2003.

⁹⁵ NetScreen Security Advisory, 57739, July 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Network Associates ⁹⁶	Windows NT 4.0/2000, 2003	McAfee ePolicy Orchestrator 2.0, 2.5, SP1, 2.5.1	Multiple vulnerabilities exist: a vulnerability exists when processing POST requests of excessive length due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; and a format string vulnerability exists in the processing of the 'ComputerList' parameter, which could let a remote malicious user execute arbitrary code.	Patches available at: http://download.nai.com/products/patches/ePO/v2.x/	ePolicy Orchestrator POST Request & ComputerList Parameter CVE Names: CAN-2003-0149, CAN-2003-0616	High	Bug discussed in newsgroups and websites.
Network Associates ⁹⁷	Windows NT 4.0/2000, 2003	McAfee ePolicy Orchestrator 2.0, 2.5, SP1, 2.5.1, 3.0	A vulnerability exists because the password is encrypted with a secret key that is stored in a DLL on the system, which could let a remote malicious user obtain administrative privileges.	Patches available at: http://download.nai.com/products/patches/	ePolicy Orchestrator MSDE SA Account CVE Name: CAN-2003-0148	High	Bug discussed in newsgroups and websites.
Network Associates ⁹⁸	Windows NT 4.0/2000, 2003	McAfee ePolicy Orchestrator 3.0	A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information.	Patches available at: http://download.nai.com/products/patches/ePO/v3.0/EPO3002.Zip	ePolicy Orchestrator Directory Traversal CVE Name: CAN-2003-0610	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

⁹⁶ @stake, Inc. Security Advisory, a073103-1, July 31, 2003.

⁹⁷ @stake, Inc. Security Advisory, a073103-1, July 31, 2003.

⁹⁸ Network Associates Security Bulletin, July 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
nfs ^{99, 100, 101, 102, 103, 104, 105, 106} <i>More upgrades issued^{107, 108}</i>	Unix	nfs-utils 0.2, 0.2.1, 0.3.1, 0.3.3, 1.0, 1.0.1, 1.0.3	A buffer overflow vulnerability exists due to a boundary error (off-by-one) in the 'xlog()' function when adding missing trailing newlines to a logged string, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=14&release_id=171379 Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/n/nfs-utils/ Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/nfs-utils-0.3.1-7_imnx_3.i386.rpm Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/ Slackware: ftp://ftp.slackware.com/pub/slackware/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.net/pub/Trustix/updates/ Sun: http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert%2F55882 YellowDog: ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/	NFS-Utills Xlog Remote Buffer Overflow CVE Name: CAN-2003-0252	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

⁹⁹ Debian Security Advisory, DSA 349-1, July 14, 2003.

¹⁰⁰ Red Hat Security Advisory, RHSA-2003:206-01, July 14, 2003.

¹⁰¹ Slackware Security Advisory, SSA:2003-195-01, July 15, 2003.

¹⁰² Immunix Secured OS Security Advisory, IMNX-2003-7+-018-01, July 15, 2003.

¹⁰³ Trustix Secure Linux Security Advisory, TLSA-2003-0027, July 18, 2003.

¹⁰⁴ SuSE Security Announcement, SuSE-SA:2003:031, July 16, 2003.

¹⁰⁵ Mandrake Linux Security Update Advisory, MDKSA-2003:076, July 21, 2003.

¹⁰⁶ Conectiva Linux Security Announcement, CLA-2003:700, July 22, 2003.

¹⁰⁷ Yellow Dog Linux Security Announcement, YDU-20030718-1, July 18, 2003.

¹⁰⁸ Sun(sm) Alert Notification, 55882, July 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell ¹⁰⁹	Multiple	iChain Server 2.1, SP1&SP2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists when a special script is run against the login, which could let a remote malicious user cause a Denial of Service; and a buffer overflow vulnerability exists when excessive data is passed as a user login name, which could let a remote malicious user cause a Denial of Service.	Service pack available at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966560.htm	Multiple Novell iChain Buffer Overflow Denial of Service	Low	Bug discussed in newsgroups and websites.
Novell ¹¹⁰	Multiple	Groupwise 6.5, GroupWise WebAccess 6.5	A vulnerability exists due to the way user passwords are handled, which could let a malicious user obtain sensitive information.	Upgrades available at: http://support.novell.com/finder/	GroupWise Wireless Webaccess Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Novell ¹¹¹	Multiple	Border Manager 3.7, 3.7 SP1	Multiple vulnerabilities exist including lack of adequate filtering of certain types of traffic such as: TCP Push Attacks, attempts to exploit FTP PASV issues, and attacks which rely on repeated ICMP error replies being sent through the firewall; and insufficient facilities for logging HTTPS traffic or certain ICMP messages, which could let some types of traffic bypass detection and filtering.	Upgrades available at: http://support.novell.com/ser/vlet/filedownload/sec/pub/bm37sp2.exe	Border Manager Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Oyvind Gronnesby, ¹¹²	Unix	mod_mylo 0.1, 2.0, 2.1	A buffer overflow vulnerability exists in the logging section due to insufficient bounds checking on HTTP requests, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.pvv.ntnu.no/~oyving/code/mod_mylo/mod_mylo-0.2.2.tar.gz	Mod_Mylo Apache Module REQSTR Remote Buffer Overflow CVE Name: CAN-2003-0651	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
PBLang ¹¹³	Windows, Unix	PBLang 4.0	A Cross-Site Scripting vulnerability exists in the 'docs.php' script, which could let a remote malicious user execute HTML and script code.	No workaround or patch available at time of publishing.	PBLang Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

¹⁰⁹ Secunia Security Advisory, July 28, 2003.

¹¹⁰ Novacoast Security Advisory, July 31, 2003.

¹¹¹ SecurityFocus, July 30, 2003.

¹¹² CLIVITT-2003-5 Advisory, July 28, 2003.

¹¹³ Bugtraq, July 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PBLang ¹¹⁴	Windows, Unix	PBLang 4.0 PBLang 4.56 (4.5 RC 2)	A vulnerability exists because users can include '<>' in their postings, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	PBLang Bulletin Board System IMG Tag HTML Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHP Arena ¹¹⁵	Unix	paFileDB 1.1.3, 2.1.1, 3.0 Beta 3.1, 3.0, 3.1	A vulnerability exists in the '/includes/team/file.php' script due to insufficient verification of user credentials before accepting files for upload, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.phparena.net/downloads/pafiledb.php?action=file&id=16	paFileDB Arbitrary File Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.
PHP Group Ware ¹¹⁶ <i>Patches now available 117, 118</i> <i>Debian issues patches</i> ¹¹⁹	Windows, Unix	PHPGrou pWare 0.9.14 .003	Multiple Cross-Site Scripting vulnerabilities exist in the form fields due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code.	<i>Patches available at:</i> http://www.phpgroupware.org/downloads/Conectiva: http://www.mandrakesecurity.net/en/ftp.php <i>Debian:</i> http://security.debian.org/pool/updates/main/p/phpgroupware/	Multiple PHPGroup Ware HTML Injection	High	Bug discussed in newsgroups and websites. There is no exploit code required.
PHP-Gastebuch ¹²⁰	Windows, Unix	PHP-Gastebuch 1.60 Beta	A vulnerability exists in the 'guestbookdat' file and the 'pwd' password file due to insufficient access controls, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Multiple PHP-Gastebuch Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹¹⁴ Bugtraq, July 27, 2003.

¹¹⁵ Bugtraq, July 24, 2003.

¹¹⁶ Kereval Security Advisory, KSA-003, July 2, 2003.

¹¹⁷ Conectiva Linux Security Announcement, CLA-2003:697, July 16, 2003.

¹¹⁸ Mandrake Linux Security Update Advisory, MDKSA-2003:077, July 23, 2003.

¹¹⁹ Debian Security Advisory, DSA 365-1, August 6, 2003.

¹²⁰ Zone-h Security Team Advisory, ZH2003-12SA, July 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpMy Admin¹²¹ <i>Upgrades now available¹²²</i>	Windows, Unix	phpMy Admin 2.0-2.0.5, 2.1-2.2.6, 2.3.1, 2.3.2, 2.4.0, 2.5.0, 2.5.1	Multiple vulnerabilities exist: Several Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; a Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information; a path disclosure vulnerability exists, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because passwords are stored in a plaintext format, which could let a malicious user obtain sensitive information.	<i>Upgrade available at: http://www.phpmyadmin.net/index.php?dl=2</i>	PHPMyAdmin Multiple Cross-Site Scripting	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required for the Cross-Site Scripting, path disclosure, & plaintext password vulnerabilities. Proof of Concept exploit has been published for the Directory Traversal vulnerability.
Quality On Line Ltd.¹²³ <i>Upgrade now available¹²⁴</i>	Windows	IRCXpro Server 1.0	A vulnerability exists in the 'settings.ini' file due to the method used for password storage, which could let a malicious user obtain unauthorized access.	<i>Upgrade available at: http://www.ircxpro.com/default.asp?id=download</i>	IRCXpro Server 'Settings.INI' Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
RAV AntiVirus¹²⁵	Multiple	Online Virus Scan	A buffer overflow vulnerability exists in the 'update()' function when excessive data is submitted as an internal function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Online Virus 'update()' Function Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Roundup¹²⁶	Unix	Roundup 0.5-0.5.7	A Cross-Site Scripting vulnerability exists in 'clinet.py' due to missing validation of input passed through CGI variables, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=31577&release_id=172354	Roundup 'Client.PY' Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹²¹ Advisory: NSRG-15-7, June 18, 2003.

¹²² SecurityFocus, July 24, 2003.

¹²³ Exploitlabs.com Advisory 002, June 3, 2003.

¹²⁴ SecurityFocus, July 25, 2003.

¹²⁵ Bugtraq, August 1, 2003.

¹²⁶ SecurityTracker Alert, 1007327, July 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SGI ¹²⁷	Unix	IRIX 6.5-6.5.21, 6.5.17 m-6.5.21 m, 6.5.17 f-6.5.21 f	A buffer overflow vulnerability exists in the Name Service Daemon (nsd) software in the RPC AUTH_UNIX implementation, which could let a remote malicious execute arbitrary code with root privileges.	Patch details and upgrade instructions available at: ftp://patches.sgi.com/support/free/security/advisories/20030704-01-P	IRIX Name Service Daemon Buffer Overflow CVE Name: CAN-2003-0575	High	Bug discussed in newsgroups and websites.
Softshoe ¹²⁸	Multiple	Softshoe	A Cross-Site Scripting vulnerability exists in the 'Parse-file' script due to insufficient filtering of HTML or script code, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Softshoe Parse-file Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required however, an exploit has been published.
Stanley T. Shebs ¹²⁹	Unix	Xconq 7.4.1	A buffer overflow vulnerability exists in the 'make_default_player_spec()' function due to insufficient bounds checking of data supplied via the USER and DISPLAY environment variables, which could let a malicious user execute arbitrary code.	<u>Debian:</u> http://security.debian.org/pool/updates/main/x/xconq/	XConq 'make_default_player_spec()' Buffer Overflow CVE Name: CAN-2003-0607	High	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc. ¹³⁰	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A buffer overflow vulnerability exists in the ld runtime linker due to insufficient bounds checking performed in the routines used to process the value of LD_PRELOAD, which could let a malicious user execute arbitrary code with root privileges.	Patches available at: http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert/55680	Solaris Runtime Linker Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Sun Microsystems, Inc. ¹³¹	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A Denial of Service vulnerability exists in the 'PSIG' kernel function.	Patches available at: http://sunsolve.sun.com	Solaris PSIG Denial of Service	Low	Bug discussed in newsgroups and websites.

¹²⁷ SGI Security Advisory, 20030704-01-P, July 29, 2003.

¹²⁸ SecurityFocus, July 28, 2003.

¹²⁹ Debian Security Advisory, DSA 354-1, July 29, 2003.

¹³⁰ iDEFENSE Security Advisory, July 29, 2003.

¹³¹ Sun(sm) Alert Notification, 47353, July 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Microsystems, Inc. ¹³²	Unix	ONE Application Server 6.5, SP1 MU1, SP1, MU1	A vulnerability exists due to an unspecified error allowing the source code of Java Server Pages (".jsp") to be disclosed, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.sun.com/software/download/products/3eea8309.html	ONE Application Server Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Symantec ¹³³	Windows 98/ME/NT 2.0/2000, XP	Norton AntiVirus 2002, 2003	A vulnerability exists due to an error in the 'DeviceIoControl()' function, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Norton AntiVirus 'DeviceIoControl()' Function	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Symantec ¹³⁴	Windows NT 4.0/2000, XP	Quarantine Server 2.6, 3.2, 3.11; Norton AntiVirus Corporate Edition version 7.61	A remote Denial of Service vulnerability exists due to an error in 'qserver.exe' when handling connections to the TCP listener port.	Upgrades available at: http://securityresponse.symantec.com/avcenter/security/Content/2003.07.29.html	Quarantine Server Denial of Service	Low	Bug discussed in newsgroups and websites.
University of Minnesota ¹³⁵	Unix	gopherd 2.0.3, 2.0.4 2.3, 2.3.1, 3.0.0- 3.0.5	A buffer overflow vulnerability exists in the 'do_command()' function due to insufficient verification, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GopherD Do_Command Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Valve Software ¹³⁶	Windows 98/NT 4.0	Half-Life 1.1 .0.8, 1.1.0.9, 1.1.1.0	A buffer overflow vulnerability exists in the client connection routine due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Half-Life Client Connection Routine Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

¹³² Sun(sm) Alert Notification, 56020, August 5, 2003.

¹³³ Securiteam, August 4, 2003.

¹³⁴ Qualys Security Research Team. Advisory, July 28, 2003.

¹³⁵ Securiteam, July 24, 2003.

¹³⁶ Securiteam, July 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Valve Software ¹³⁷	Windows 98/ME/NT 4.0/2000, Unix	Half-Life 1.1 .0.8, 1.1.0.9, 1.1.0.4 Windows, 1.1.0.4 Linux, 1.1.1.0, Half-Life Dedicated Server 3.1.1.1c1 Linux, 4.1.1 .1a Win32	Two vulnerabilities exist: a buffer overflow vulnerability exists due to insufficient bounds checking of client-supplied data during requests to join multiplayer games, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability exists due to an input validation error during requests to join multiplayer games.	Upgrade available at: ftp://ftp.valvesoftware.com/Linux/hlds_1_3111d_update.tar.gz ftp://ftp.valvesoftware.com/Win32/hlds4111d_beta.exe	Half-Life Dedicated Server Multiplayer Request Buffer Overflow & Denial of Service	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit scripts have been published.
VBulletin ¹³⁸	Windows	VBulletin 3.0 beta 2	A vulnerability exists in the 'register.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	VBulletin 'Register.PHP' Code Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.
VM Ware, Inc. ¹³⁹ <i>Upgrade now available</i> ¹⁴⁰	Unix	GSX Server 2.5.1, VMWare Workstation 4.0	A vulnerability exists because environment variables may be manipulated, which could let a malicious user execute arbitrary code and obtain root access.	Patch available at: http://www.vmware.com/vmwarestore/newstore/download.jsp?ProductCode=GSX-LX-ESD <i>Upgrade available at:</i> http://www.vmware.com/support/ws3/doc/upgrade_ws.html	VMware GSX Server/ Workstation Host Operating System Compromise	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹³⁷ Bugtraq, July 29, 2003.

¹³⁸ SecurityFocus, August 6, 2003.

¹³⁹ Bugtraq, July 26, 2003.

¹⁴⁰ SecurityFocus, August 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Wietse Venema 141, 142, 143, 144, 145, 146, 147	Unix	Postfix 20011115, 20010228, 19991231, 19990906, 1.0.21, 1.1.11- 1.1.13	Multiple remote Denial of Service vulnerabilities exist: a vulnerability exists that allows a remote malicious user to 'bounce-scan' a private network and use the server as a Distributed Denial of Service tool; and a remote Denial of Service vulnerability exists when a remote malicious user submits a malformed envelope address.	Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/p/postfix/ Engarde: http://infocenter.guardiandigital.com/advisories/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/ SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.net/pub/Trustix/updates	Multiple Postfix Denial of Service CVE Names: CAN-2003-0468, CAN-2003-0540	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Wolflab ¹⁴⁸	Windows, Unix	MOD Guthabenhack 1.3	An input validation vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	MOD Guthabenhack Input Validation	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
XBlast ¹⁴⁹	Unix	XBlast 2.6.1	A buffer overflow vulnerability exists in the 'HOME' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	XBlast 'HOME' Environment Variable Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
xfstt ¹⁵⁰ <i>Debian issues advisory 151</i>	Unix	xfstt 1.4	A memory corruption vulnerability exists which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Debian: http://security.debian.org/pool/updates/main/x/xfstt/	xfstt Memory Corruption CVE Name: CAN-2003-0625	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹⁴¹ Conectiva Linux Security Announcement, CLA-2003:717, August 4, 2003.

¹⁴² Debian Security Advisory, DSA 363-1, August 4, 2003.

¹⁴³ Guardian Digital Security Advisory, ESA-20030804-019, August 4, 2003.

¹⁴⁴ Mandrake Linux Security Update Advisory, MDKSA-2003:081, August 4, 2003.

¹⁴⁵ Red Hat Security Advisory, RHSA-2003:251-01, August 4, 2003.

¹⁴⁶ SuSE Security Announcement. SuSE-SA:2003:033, August 4, 2003.

¹⁴⁷ Trustix Secure Linux Security Advisory, TSLSA-2003-0029, August 7, 2003.

¹⁴⁸ BadWebMasters Security Advisory, #015, July 31, 2003.

¹⁴⁹ 0x333 Outsiders Security Labs Security Advisory, July 23, 2003.

¹⁵⁰ SecurityFocus, July 23, 2003.

¹⁵¹ Debian Security Advisory, DSA 360-1, August 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
xfstt ¹⁵² <i>Debian issues advisory</i> ¹⁵³	Unix	xfstt 1.4	A buffer overflow vulnerability exists in the TrueType Font Server for X11 (xfstt) due to a boundary error in the "working()" function, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	<u>Debian:</u> http://security.debian.org/pool/updates/main/x/xfstt/	xfstt Remote Buffer Overflow CVE Name: CAN-2003-0581	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Zone Labs ¹⁵⁴	Windows 95/98/ME/NT 4.0/2000, XP	ZoneAlarm 2.1-2.6, 3.0, 3.1	A buffer overflow vulnerability exists due to an error in the TrueVector Device Driver ("vsdatant.sys"), which could let a malicious user execute arbitrary code.	The vendor has acknowledged this issue and stated that a fix is pending. Registered ZoneAlarm users may be notified when updates are available by enabling the "Check for Update" feature in the software.	ZoneAlarm TrueVector Device Driver	High	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between July 23 and August 6, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 49 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

¹⁵² ERA IT Solutions Security Advisory, July 14, 2003.

¹⁵³ Debian Security Advisory, DSA 360-1, August 1, 2003.

¹⁵⁴ Sec-labs Team Advisory, August 5, 2003.

Date of Script (Reverse Chronological Order)	Script name	Script Description
August 6, 2003	oc192-dcom.c	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability. This exploit uses ExitThread in its shellcode to prevent the RPC service from crashing upon successful exploitation.
August 6, 2003	xmandb.sh	Exploit for the ManDB Compressor Binary Elevated Privileges vulnerability.
August 6, 2003	wu262.zip	Remote root exploit for the Wuftpd Off-by-one vulnerability.
August 5, 2003	07.30.dcom48.c	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability.
August 5, 2003	0x82-dcomrpc_usemgret.c	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability.
August 5, 2003	0x82-wu262.c	Script that exploits the Multiple Vendor realpath() Off-By-One Buffer Overflow vulnerability.
August 5, 2003	dcomworm.zip	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability.
August 5, 2003	DominoHunter-0.91.zip	A Lotus Domino web server scanner, written in Perl, that attempts to access default NSF databases, as well as crawl user-defined bases. It tries to enumerate the database structure, enumerate available views, available documents, and ACLs set on documents.
August 5, 2003	everybuddy-dos.pl	Perl script that exploits the EveryBuddy Long Message Remote Denial of Service vulnerability.
August 5, 2003	jmpreg.zip	jmpreg is a python class that makes it easy to find jmp calls inside various Windows DLLs. This class is especially helpful for local overflows.
August 5, 2003	Poc.c.txt	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability.
August 5, 2003	postfix.pl	Perl script that exploits the Postfix Remote Denial of Service vulnerability.
August 5, 2003	postfixdos.c	Script that exploits the Postfix Remote Denial of Service vulnerability.
August 5, 2003	priv8-uhagr-halflife.c	Script that exploits the Half-Life Client Connection Routine Remote Buffer Overflow vulnerability.
August 5, 2003	ShatterMaster.zip	A win32 program written in VB6 to develop and exploit shatter attacks in Windows NT/2k/XP.
August 5, 2003	SRT2003-08-01-0126.txt	Instructions for exploiting the CDRTools RSCSI Debug File Arbitrary Local File Manipulation vulnerability.
August 5, 2003	xtokkax.c	Script that exploits the Xtokkaetama Nickname Buffer Overflow vulnerability.
August 4, 2003	0x82-WOOoou~Happy_new.c	Exploit for the Multiple Vendor realpath() Off-By-One Buffer Overflow vulnerability
August 4, 2003	NAVAP_EXPLOIT.ASM	Exploit for the Norton AntiVirus 'DeviceIo Control()' Function vulnerability.
August 3, 2003	xtokkax.c	Script that exploits the Xtokkaetama Nickname Buffer Overflow vulnerability.
August 3, 2003	xtama.c	Script that exploits the Xtokkaetama Nickname Buffer Overflow vulnerability.
August 2, 2003	30.07.03.dcom.c	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability.
August 2, 2003	dcomrpc.c	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability.
July 30, 2003	suiddmp.c	Exploit for the Linux 2.4 execve() system call Denial of Service vulnerability.
July 29, 2003	0x333-lockdexvul.txt	Exploit for the lockdex vulnerability.
July 29, 2003	CLIVITT-2003-5.txt	Exploit for the Mod_Mylo Apache Module REQSTR Remote Buffer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 29, 2003	dcomsploit.tgz	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability.
July 29, 2003	hlbof-client.zip	Exploit for the Half-Life Dedicated Server Multiplayer Request Buffer Overflow & Denial of Service vulnerabilities.
July 29, 2003	hlbof-server.zip	Exploit for the Half-Life Dedicated Server Multiplayer Request Buffer Overflow vulnerability.
July 29, 2003	knfsd_dos.c	Script that exploits the Linux Kernel 2.4 'nfsexdr.c' Remote Denial of Service vulnerability.
July 29, 2003	pu-hl.c	Exploit for the Half-Life Dedicated Server Multiplayer Request Buffer Overflow vulnerability.
July 29, 2003	shatterSEH2.txt	Version two that discusses more shatter attacks which are possible using SEH memory locations to escalate privileges in Windows. Exploit code included.
July 29, 2003	sqlscan12eval.zip	SQLScan v1.2 is intended to run against Microsoft SQL Server and attempts to connect directly to port 1433. It features the ability to scan one host or an IP list from an input file, the ability to scan for one SQL account password or multiple passwords from a dictionary file, and the ability to create an administrative NT backdoor account on vulnerable hosts.
July 28, 2003	imapd_overflow	Description of a simple buffer overflow attack against older IMAP servers developed by the University of Washington.
July 28, 2003	mod_mylo_exploit.c	Script that exploits the Mod_Mylo Apache Module REQSTR Remote Buffer Overflow vulnerability.
July 28, 2003	msqlcx.c	Script that exploits the Mini SQL Remote Format String vulnerability.
July 28, 2003	nsniff-0.1.2.tar	Packet capturing and network monitoring tool that contains all the basics for monitoring network traffic.
July 28, 2003	zappa-0.2.c	A backdoor that waits for an ICMP packet and then connects with a UDP server on the client.
July 27, 2003	benjurry.txt	Thorough analysis of the buffer overrun in the Windows RPC interface and exploit for Windows 2000 SP4 Chinese version.
July 27, 2003	dcom.c	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability.
July 27, 2003	DComExpl_UnixWin32.zip	Script that exploits the Windows DCOM RPC Buffer Overflow vulnerability.
July 27, 2003	Gobbler-2.0.1-Alpha1.tar.gz	Gobbler is a tool designed to audit various aspects of DHCP networks, from detecting if DHCP is running on a network to performing Denial of Service attack. Gobbler also exploits DHCP and Ethernet, to allow distributed spoofed port scanning with the added bonus of being able to sniff the reply from a spoofed host.
July 27, 2003	illmob.txt	Paper discussing utilization of the Win32 exploit for the DCOM RPC vulnerability.
July 27, 2003	ippcheck-0.1.6.tar	Scans an IP range and checks if a specified port is open for TCP connections. Can also search for specific parts in strings that the servers return.
July 27, 2003	nsniff-20021019.tar	Packet capturing and network monitoring tool that contains all the basics for monitoring network traffic.
July 27, 2003	sambash-release.c	Remote root exploit for samba 2.2.7a and below using reply_nttrans().
July 27, 2003	zappa.c	An advanced backdoor which waits for a ICMP packet and then connects to a UDP server on the client. H
July, 25, 2003	SACscan.tar.gz	A basic portscanner that is like Nmap.
July 23, 2003	0x333xbblast.c	Script that exploits the XBlast 'HOME' Environment Variable Buffer Overflow vulnerability.

Trends

- The DHS/Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) has issued a second update to the security advisory on Microsoft's DCOM RPC Buffer Overflow vulnerability. Malicious code dubbed "MSBLAST," "LOVSCAN," or "BLASTER" began circulating on the Internet on August 11th. (Additional information regarding this worm can be found in the "Virus" section.) This worm takes advantage of the vulnerability discussed in Microsoft's advisory located at: <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp> and contains code that will target Microsoft's update servers on August 16th. This additional attack could cause significant Internet-wide disruptions. It is also possible that other worms based on this vulnerability will be released over the next few days as "copy cat" attacks. Also numerous exploits and Trojans have been reported in the wild that exploit this vulnerability. Please ensure that you have applied the Microsoft patch for this vulnerability.
- The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) is receiving reports of a new mass mailing virus, now referred to as W32/Mimail, spreading on the Internet. For more information see Department of Homeland Security Advisory located at: <http://www.nipc.gov/warnings/advisories/2003/W328022003.htm> and "Virus" and "Trojan" sections.
- Online vandals are using a program to compromise Windows servers and remotely control them through Internet relay chat (IRC) networks. Several programs, including one that exploits a recent vulnerability in computers running Windows, have been cobbled together to create a remote attack tool. The tool takes commands from an attacker through the IRC networks and can scan for and compromise computers vulnerable to the recently discovered flaw in Windows
- The CERT/CC has received reports of systems being compromised by two recently discovered vulnerabilities in the Microsoft Remote Procedure Call (RPC) service. Additionally, the CERT/CC has received reports of widespread scanning for systems with open Microsoft RPC ports (135, 139, 445). For more information, see "Exploitation of Microsoft RPC Vulnerabilities" located at: <http://www.cert.org/current/>.
- The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting a vulnerability in popular Microsoft Windows operating systems. DHS expects that exploits are being developed for malicious use. For more information see, "Bugs, Holes & Patches" Table "Windows DCOM RPC Buffer Overflow" and DHS/IAIP Advisory located: <http://www.nipc.gov/warnings/advisories/2003/Potential72403.htm>. Additional information on the Microsoft vulnerability may also be found at: <http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>.
- The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) has issued an advisory to heighten awareness of a remotely exploitable vulnerability in Cisco IOS 10.3 or later. The recently announced vulnerability in devices running Cisco IOS 10.3 or later may be exploited to cause a Denial of Service state. Because routers and switches are an essential part of all network infrastructures, and because Cisco devices comprise a significant portion of those infrastructures, widespread exploitation of vulnerable Cisco devices could disrupt portions of the Internet. For more information see "Bugs, Holes & Patches" Table and DHS/FedCIRC Advisory FA-2003-15 located at: <http://www2.fedcirc.gov/advisories/FA-2003-15.html>.
- Recent reports to the CERT/CC have highlighted two chronic problems:
 - The speed at which viruses are spreading is increasing. This echoes the trend toward faster propagation rates seen in the past few years in self-propagating malicious code (i.e., worms). A similar trend from weeks to hours has emerged in the virus (i.e., non-self-propagating malicious code) arena.

- In a number of the reports, users who were compromised may have been under the incorrect impression that merely having antivirus software installed was enough to protect them from all malicious code attacks. This is simply a mistaken assumption, and users must always exercise caution when handling e-mail attachments or other code or data from untrustworthy sources. For more information see, CERT® Incident Note IN-2003-01, located at: http://www.cert.org/incident_notes/IN-2003-01.html.

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available.** The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Klez	Worm	Slight Increase	January 2002
2	W32/Bugbear	File	Slight Decrease	September 2002
3	W32/Mimail	Worm	New to Table	July 2003
4	W32/Sobig	Worm	Slight Decrease	May 2003
5	W32/Yaha	Worm	Slight Decrease	February 2002
6	Elkern	File Infector	Increase	October 2001
7	Funlove	File	Slight Decrease	November 1999
8	W32/Lovegate	Virus	Decrease	February 2003
9	W32/SQLSlammer	Worm	Stable	January 2003
10	W32/Fizzer	Worm	Stable	May 2003

Note: Note: Virus reporting may be weeks behind the first discovery of infection. A total 212 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 320 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Bat/Boohoo-A (Aliases: Bat.NTScan.A, Bat.IROffer12.A, Bat/Mumu, BAT/Mumu.worm.c) (Batch File Worm): This is an Internet worm that spreads via weakly protected network shares on Windows computers. The worm generates random IP numbers and uses a network scanner to scan these IP ranges for vulnerable computers. The worm consists of the following files:

- starter.bat
- scan.bat
- ip.bat
- hacker.bat
- Xecuter.bat

- regkeyadd.REG

and various benign files. These files are copied to the Windows system32 folder on the remote compromised computer. The subfolders, tmp and tmp1, are created inside the Windows system32 folder on the remote machine and the hidden attribute is set on the system32 folder. After the files are copied, the worm is started remotely. The worm starts the following services:

- startupdll (startup script psexec.bat)
- msnet (svhost.exe)
- drvmanager (drvquery32.exe)
- serv-u (drvquery32.exe)

Bat/Boohoo-A attempts to delete all LOG files from the root folders of drives C: and D: and uses the included clearlogs.exe application to clean system log files. The worm also attempts to remove the shares C\$ to Z\$. It creates backup copies of several of its files. In order to run automatically on system startup, Bat/Boohoo-A sets the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run:
drvmanager = "C:\\winnt\\system32\\drvquery32.exe /S"
HideRun.exe = "C:\\winnt\\system32\\HideRun.exe
c:\\winnt\\system32\\svhost.exe c:\\winnt\\system32\\pro.gif"
Xecuter.bat = C:\\winnt\\system32\\psexec.bat"

The worm also sets the following network registry entries:

- HKLM\\SYSTEM\\CurrentControlSet\\Services\\lanmanserver\\parameters:
"AutoShareWks"=dword:00000000
"AutoShareServer"=dword:00000000

Harmony.A (Aliases: Win32.Xorala, W32/Harmony.A): This virus does not contain any payload, however it will attempt to infect all the EXE files it finds from the main Windows and the Windows' System folders. Upon infection, the size of the files will have been increased by 2048 bytes and the timestamp of the file will reflect the date the infection took place. The virus will add its own code in the end of the host's executable, creating for that purpose a section named XOR. The virus does not have any means of spreading by itself through networks. In order for a computer to be infected an already infected file has to be manually run.

Haver.1309 (DOS Virus): This is a DOS memory-resident virus that infects the .exe files. When a file that is infected with Haver.1309 is executed, it hooks interrupt 21h and 24h. After this occurs, the virus will infect any uninfected .exe files, which were loaded and executed. The virus attempts to overwrite the CMOS checksum if the system date is April 6th and executes the original file.

Linux/Brunfly (File Infector Virus): This is a direct action file infector, infecting ELF binary files in the current directory. Infected files have their filesize increased with (usually) 4096 bytes decimal. Visible strings inside infected files include for example: WARNING: brundle-fly infected!

WORM_MSBLAST.A (Aliases: W32/Lovsan.worm, W32/Blaster-A, W32.Blaster.Worm, Worm.Win32.Lovsan, Win32.Poza, Lovsan, W32/Blaster) (Internet Worm): This worm has been reported in the wild. It exploits the RPC DCOM BUFFER OVERFLOW. It does not use email to spread. Targeted computers include the following Microsoft operating systems:

- Windows NT 4.0
- Windows NT 4.0 Terminal Services Edition
- Windows 2000
- Windows XP
- Windows Server 2003

(On Windows XP the exploit can accidentally cause the remote RPC service to terminate. This causes the Windows XP machine to reboot). Windows 95/98/ME computers, which don't run an RPC service nor have a TFTP client (default setting), are not at risk. On finding a vulnerable computer system, the worm causes the remote machine to acquire a copy of the worm using TFTP, which is saved as msblast.exe in the Windows system folder. Microsoft issued a patch for the vulnerability exploited by this worm on July 16, 2003. The patch is available from:

- <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>

From 16 August 2003, one month after the security patch was posted, the worm is programmed to launch a Distributed Denial of Service (DDoS) attack on windowsupdate.com, which may severely impact access to the website Microsoft uses to distribute security patches. Additionally the worm creates the following registry entry so as to run on system start:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\windows auto update

The worm contains the following text, which does not get displayed:

- I just want to say LOVE YOU SAN!! billy gates why do you make this possible ? Stop making money and fix your software!!

It has been observed to continuously scan random IP addresses and send data to vulnerable systems on the network using port 135. This worm attempts to download the msblast.exe file to the %WinDir%\system32 directory and execute it. It also attempts to block access to TCP port 4444 at the firewall level, and then blocks the following ports, if they do not use the applications listed:

- TCP Port 135, "DCOM RPC"
- UDP Port 69, "TFTP"

VBS.Bingd@mm (Aliases: Trojan.VBS.NoExp, VBS/Generic@MM) (Visual Basic Script Worm):

This is a mass-mailing worm that spreads using Microsoft Outlook. It modifies the registry and sends itself to the first seven addresses in the Microsoft Outlook Address Book. It is written in Visual Basic Script.

W32.Babybear.int (Win32 Worm): This is an intended mass-mailing worm that is a variant of W32.Babybear@mm. When this worm is run, it may display a fake message titled "Microsoft Windows Update." This threat is written in the Microsoft Visual Basic (VB) programming language. The VB run-time libraries are required to execute W32.Babybear.int.

W32/Cidu-A (Win32 Virus): This virus is written in Delphi. When you run an infected program, W32/Cidu-A searches your hard disk for EXE (program) files, and overwrites each program it finds with a copy of itself. It attempts to make a copy of the original program first, using the original name with the extension .DLL added. But the virus sometimes fails to copy the original program, creating instead a zero-byte file. This makes the virus very noticeable, as programs destroyed in this way (rather obviously) do not work any more. It marks infected files hidden, system and read-only. It also adds a registry entry of the form:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\OriginalFileName

for each infected file. As a payload, W32/Cidu-A activates the tray of your CD-ROM drive, displays and then removes a picture of a black dog merged with a human face, removes and possibly replaces your Desktop icons, disables your taskbar, and disables your keyboard or mouse.

W32.Earlybird@mm (Alias: I-Worm.Wormex): This is a mass-mailing worm that mails itself to all the addresses in the Microsoft Outlook Address Book. It spreads via the file-sharing applications, KaZaA and eDonkey and if the host is running IIS or Apache, attempts to set itself up in the root directory of the Web server. The worm is written in Delphi.

W32/Gruel-M IWin32 Worm): This is a mass mailing worm very similar to the other variants in this family.

W32.HLLW.Huntocx (Win32 Worm): The W32.HLLW.Huntocx worm attempts to spread itself through IRC and file-sharing programs, such as KaZaA and KaZaA Lite. It also attempts to terminate the processes of various antivirus and security programs, and then drops itself into the system folder. The virus continues to run in the background, acting as an IRC backdoor.

W32.HLLW.Gotorm (Win32 Worm): This is a worm that steals sensitive information from some video games and attempts to spread through the KaZaA file-sharing network. When W32.HLLW.Gotorm is executed, it displays the fake error message, titled "Win Zip Self-Extractor."

W32.HLLW.Niklas (Aliases: Worm.P2P.Niklas, W32/MScr.worm!p2p): This is a worm that attempts to spread across file-sharing networks, such as KaZaA, Morpheus, and eDonkey2000. The worm prepends itself to executables it locates in certain folders. It will attempt to terminate the processes of various programs, including antivirus and firewall software. W32.HLLW.Niklas is a Delphi application, packed with UPX 1.08, Yoda's Crypter 1.2.

W32.Kergez.A@mm (Alias: I-Worm.Kergez) (Win32 Worm): This is a mass-mailing worm that sends itself to all the e-mail addresses that it finds in the following files:

- Files with the *.asp, *.ht* extensions.

Files located in any of the directories specified in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders.

The e-mail messages will have various subjects and attachments. The worm attempts to terminate the processes of various programs, including antivirus software. W32.Kergez.A@mm is written in Microsoft Visual C++ and is UPX-packed.

W32.Liamed@mm (Win32 Worm): This is a mass-mailing worm that uses its own SMTP engine to send itself to all the contacts in Microsoft Windows Address Book. It has backdoor functionality that can download files from the Internet and e-mail stolen information to the author of the worm. The subject line and the message body of the e-mail use Chinese characters, and the attachment is titled "hello.exe." The worm is written in the Microsoft C++ programming language and is compressed with UPX.

W32/Lovgate-L (Win32 Worm): This worm has been reported in the wild. It is functionally similar to W32/Lovgate-J except that this variant copies itself to the Windows system folder as WINEXE.EXE and changes the following registry entry so that WINEXE.EXE is run before an EXE file:

- HKCR\exefile\shell\open\command

W32.Lorsis.Worm (Win32 Worm): This is a worm that spreads through the KaZaA file-sharing network. If this worm is executed in February, or from December 6 to 31, it deletes critical system files. The worm uses several different filenames ending with ".exe" (there are 15 spaces before the .exe extension). During execution, the worm repeatedly attempts to copy itself to the A: drive, resulting in noticeable noise from the floppy drive, if one is installed. W32.Lorsis.Worm is written in Visual Basic and is compressed with Aspack and UPX.

W32/Mimail-A (Aliases: W32.Mimail.A@mm WORM_MIMAIL_A, W32/Mimail@MM, Mimail, Win32.Mimail.A, I-Worm.Mimail) (Win32 Worm): This worm has been reported in the wild. It arrives with the following characteristics:

- Subject line: your account <random letters>
- Attached file: message.zip

W32/Mimail-A spoofs the "From" field of the sent e-mails using the e-mail address admin@<your domain>. Inside the message.zip compressed file, is another file called message.html. If this file is opened, the worm will copy itself to C:\<Windows>\exe.tmp and C:\<Windows>\videodrv.exe. It exploits a known security vulnerability. A patch has been available from Microsoft for some months which reportedly fixes the vulnerability. W32/Mimail-A adds the following entry to the registry to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\VideoDriver
=C:\<Windows>\videodrv.exe

The worm looks for e-mail addresses in files on the local drive. It attempts to exclude various extensions from its search. It places the e-mail addresses it finds in the file C:\<Windows>\eml.tmp.

W32/Randon-R (Aliases: Worm.Win32.Randon.n, BAT_RANDOM.N, IRC/Flood.bi) (Win32 Worm): This is a network worm. When run, the worm creates numerous files in the folder C:\Windows\System\msdtc\trace. It adds the following registry entry to run the file msmngr32.exe when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\msmanager32

W32/Randon-R searches the local network for computers with weak or no passwords on the administrator or admin accounts to which it can copy itself.

W32.Simic.Worm (Alias: I-Worm.Sinmsn) (Win32 Worm): W32.Simic.Worm is a worm that spreads itself using MSN Messenger. When W32.Simic.Worm executes, it copies Sins.exe to the default MSN Messenger download folder and executes sins.exe, which downloads the following files from script.mine.nu:

- Vbdlls.exe
- Sin.dll
- Msn.exe

The worm runs Vbdlls.exe, which installs the Visual Basic run-time components on the system. It executes Msn.exe, which checks whether MSN is running, and if so, will send Sins.exe to anyone who instant messages the infected system.

W97M.Anumps.A (Word 97 Macro Virus): This is a macro virus that spreads by infecting Microsoft Word documents when they are opened or closed. It also has the ability to spread itself via IRC. While W97M.Anumps.A is active, it infects all the Microsoft Word documents that are opened or closed. Each time W97M.Anumps.A infects a new document, it disables the Word macro virus protection. It saves the newly infected document as: C:\Windows\FÁQ.doc and creates the following files:

- C:\Windows\Mumps.drv
- C:\Program Files\Microsoft Office\Office\STARTUP\Mumps.dot

The virus overwrites the file: C:\mIRC\Script.ini with a new version that will attempt to send C:\Windows\FÁQ.doc to anyone who joins or leaves any IRC channel, which the infected system is currently on. It configures Outlook Express to send C:\Windows\FÁQ.doc with every e-mail and changes the default action for the Help->About menu option in Word to display a text document (in Notepad), which contains the string:

- Windows has low memory resources. Please restart your Windows.....

and changes the background color to blue in Word.

WORM_SACHIEL.F (Aliases: W32/Sachiel.worm.f, W32.Sachiel, Worm.Win32.Sachiel.d) (Win32 Worm): This destructive worm deletes the following critical Windows files upon execution:

- REGEDIT.EXE
- MSCONFIG.EXE
- SFC.EXE

It also displays a message box. To propagate, it creates copies of itself in inserted floppy disks. This worm uses an icon commonly associated with JPEG image files. It runs on Windows 95, 98, ME, NT, 2000, and XP.

W32.Upering.Worm (Aliases: Trojan.AOL.Annoyer.b, W32/Sany.worm) (Win32 Worm): This is a mass-mailing worm that spreads by sending itself to e-mail addresses and instant message contacts in the AOL address book. It may arrive in an e-mail with an attachment named WinUpdate32Login.exe. This filename could differ depending on the original filename of the worm on the system from which the e-mail originated.

WORM_TZET.A (Aliases: W32.Tzet.Worm, Worm.Win32.Randon.u) (Internet Worm): This multi-component malware has both worm and backdoor capabilities. It propagates by penetrating systems with weak passwords and dropping a copy of itself into these vulnerable systems. It acts as a backdoor by connecting to a remote IRC server. This enables a remote malicious user to control the compromised system using IRC commands. This malware runs on Windows 95, 98, ME, NT, 2000, and XP.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.dr	dr	Current Issue
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Beasty.G	G	Current Issue
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	B	CyberNotes-2003-14
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Defcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	N/A	CyberNotes-2003-14
Backdoor.Dsklite.cli	cli	CyberNotes-2003-14
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08

Trojan	Version	CyberNotes Issue #
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Fxsvc	N/A	Current Issue
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	D	CyberNotes-2003-14
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hale	N/A	Current Issue
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Flood.F	F	Current Issue
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	Current Issue
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	N/A	CyberNotes-2003-14
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	Current Issue
Backdoor.Lala.C	C	Current Issue
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Netdevil.15	15	CyberNotes-2003-15
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nibu	N/A	Current Issue
Backdoor.Nickser	N?A	CyberNotes-2003-14
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Roxy	N/A	Current Issue
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Stealer	N/A	CyberNotes-2003-14
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Sumtax	N/A	Current Issue
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.Uzbet	N/A	CyberNotes-2003-15
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	Current Issue
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12

Trojan	Version	CyberNotes Issue #
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	Current Issue
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/PowerSpider.A	A	CyberNotes-2003-11
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader.Mimail	N/A	Current Issue
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-CY	CY	Current Issue
Downloader-DM	DM	Current Issue
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	Current Issue
IRC-BBot	N/A	Current Issue
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
JS.Seeker.J	J	CyberNotes-2003-01
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
Proxy-Migmaf	N/A	CyberNotes-2003-14
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.ALlight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	Current Issue
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09

Trojan	Version	CyberNotes Issue #
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13
QDial11	1	CyberNotes-2003-14
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Startpage-N	N	CyberNotes-2003-13
Stealther	N/A	Current Issue
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	Current Issue
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	Current Issue
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/DownLdr-DI	DI	CyberNotes-2003-15
Troj/Golon-A	A	CyberNotes-2003-15
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/QQPass-A	A	Current Issue
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	A	CyberNotes-2003-14
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
Troj/Webber-A	A	CyberNotes-2003-15
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.Ailati	N/A	CyberNotes-2003-15
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.OptixKiller	N/A	Current Issue
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	Current Issue
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Visages	N/A	CyberNotes-2003-15
Trojan.Windelete	N/A	CyberNotes-2003-14
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS.Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Bambo	N/A	CyberNotes-2003-14
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Laorenshe.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systentry.Trojan	N/A	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Woodcot	N/A	Current Issue
Xin	N/A	CyberNotes-2003-03

Backdoor.Beasty.dr (Aliases: TrojanDropper.Win32.Yabinder.a, Multidropper-CQ Trojan): This is a Trojan Horse that drops a file detected as Backdoor.Beasty.Family, executes it, and then deletes it.

Backdoor.Beasty.G (Aliases: Backdoor.BeastDoor.200.a, BackDoor-AMQ): This is a Trojan Horse that opens a listening port on your computer. It also uses web.icq.com to send a message to its creator's ICQ Unified Messaging Center, which includes the IP address of the infected computer. It is written in the Borland Delphi programming language.

Backdoor.Fxsvc (Aliases: Backdoor.Fxsvc.02, Backdoor-AQK): This is a Backdoor Trojan Horse that gives its author access to your computer. The Trojan is written in Borland Delphi and is packed with UPX. One of the payloads allows the Trojan's author to remotely shut down the compromised computer.

Backdoor.Hale (Alias: BackDoor-ATM.dr): Backdoor.Hale is a package of programs that provide backdoor access to an infected computer. This threat includes a Backdoor Trojan, detected as Backdoor.Padmin, an FTP server, and various system utilities. The existence of a C:\winnt\system32\qosrv folder is an indication of a possible infection. There have been reports that this threat is being distributed by exploiting the DCOM RPC vulnerability described in Microsoft Security Bulletin MS03-026.

Backdoor.IRC.Flood.F: This is a Backdoor Trojan Horse that will attempt to connect to an IRC server on port 6667. Once the Trojan is connected to the IRC server, it waits for commands from its creator.

Backdoor.IRC.PSK (Alias: BackDoor-AXU): This is a Trojan Horse that gives its author unauthorized access to a compromised computer. The Trojan is written in Borland Delphi and is packed with PECompact v1.50. When Backdoor.IRC.PSK is executed, it adds the value, "mssvc"="<path to trojan>," to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. The Trojan intercepts keystrokes and outputs them to a log file. Then, the Trojan will ftp this file to its creator. It also tries to connect to server irc.quake.org using port 6667, by default. This action allows the Trojan's creator unauthorized access to your machine.

Backdoor.Lala.B (Alias: BackDoor-AOT): The Trojan is a variant of Backdoor.Lala and allows unauthorized access to an infected computer. The Trojan opens TCP/UDP port 1025 to allow remote access. Backdoor.Lala.B attempts to steal confidential information (such as cached passwords and cookies), log keystrokes, and allow for remote file execution. It is written in the Borland Delphi programming language and is compressed.

Backdoor.Lala.C (Alias: BackDoor-YQ): This is a Trojan Horse that steals confidential information from a compromised computer. It is a variant of Backdoor.Lala that installs one additional file, detected as Backdoor.Trojan, to allow for remote access. The existence of the file Pntask.exe is an indication of a possible infection.

Backdoor.Nibu: This is a Trojan Horse that allows unauthorized access to an infected computer. The Trojan opens TCP port 1000, 1001, and 2283 to allow for remote access. It also attempts to steal confidential information by logging keystrokes and copying Windows password files.

Backdoor.Roxy (Aliases: Backdoor.Trojan, W32/Slanper.worm, Troj/SView-A, Worm.Win32.Randex.d, W32/Slanper.worm.gen, Win32/Slanper.B, BKDR_SONE.A): This is a backdoor Trojan which allows unauthorized remote access to the computer over a network. The Trojan adds an entry to the registry at

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- to run itself on system restart.

Backdoor.Sumtax: This is a Backdoor Trojan Horse that consists of several different utilities. Together they provide functionality to a malicious user who is commonly associated with backdoors.

Backdoor.WinShell.50 (Aliases: Backdoor.Winshell.50, BackDoor-TC): This is a server program that allows unauthorized access to an infected computer. The Backdoor will listen on port 8719. This piece of malware, along with Trojan.Stealthier, has recently been found on systems that have been exploited by the Microsoft DCOM RPC vulnerability.

Backdoor-AXR (Alias: BKDR_KOTN): There are several versions of this remote access Trojan. It connects to a URL when run leaving the machine vulnerable. The malicious user can then upload files or run scripts remotely on the infected machine. The following files are dropped by the Trojan:

- coniew.dll
- netipc32.dll
- %SYSDIR%\mswinsck.ocx

It was observed that the Trojan opened ports 3558 and 3559, however this may vary. The below key is modified to run the Trojan each time an executable is run on the system:

- HKEY_CLASSES_ROOT\exefile\shell\open\command "(Default)" = COMMGR "%1" %*

Downloader.Mimail: This is a program that downloads W32.Mimail.A@mm from a Web site, and then executes it. This appears to have been spammed to a large number of users. This program has no means of distributing itself to additional users.

Downloader-CY (Aliases: Downloader-DK, Download.Trojan.PSK, TrojanDropper.JS.Mimail.b): This downloader Trojan is created by a dropper HTML file, which was recently spammed to many e-mail addresses. That message appears as follows:

- From: Admin ADMIN@SECURITY.ORG
- Subject: Re:
- Attachment: readme.zip

The .zip file contains an HTML file, readme.html. The HTML file creates and executes Downloader-DK, with the filename aaa.exe, on vulnerable systems. This executable connects to a remote web server to download a file named ksp.exe, save it locally as mshex.exe, and execute it.

Downloader-DM (Aliases: Autorooter, Backdoor.IRC.Cirebot, Mescaline, RPC Worm, Worm.Win32.Autorooter): This is not an e-mail virus. This downloader Trojan has been found within a self-extracting dropper package (possibly named worm.exe 113,507 bytes). The self-extracting archive carries 3 files. The following files are contained within the dropper.

- rpc.exe: downloader trojan, tries to exploit MS03-026 to instruct a remote host to download lolx.exe from the infected host, via ftp, and run the downloaded exe
- rpctest.exe: MS03-026 exploit tool, creates remote shell on TCP port 57005
- tftpd.exe: haneWIN TFTP server

Other files associated with this threat are lolx.exe and dcomx.exe.

IRC-BBot: This is an IRC bot Trojan. When run, it installs itself on the local system, contacts a remote IRC server, joins a specified channel, and awaits further instruction from a malicious user. This bot contains a long list of strings to scan for various vulnerabilities. A new release of this bot was created to exploit the recent RPC Interface Buffer Overflow (7.17.03) vulnerability. When run, the Trojan installs itself as a service:

- Name: ctrmons
- Display name: Office XP Alternative User Input features.

The bot contains a keylogger, which captures typed keystrokes and Window titles to the file webcltd.dll in the WINDOWS SYSTEM (%SysDir%) directory.

IRC/Fyle: IRC/Fyle is an IRC based backdoor. Files dropped on the victim system's root and *irc directories may include: cat-penis.ini, fucking.bat, and winback.bat, having filesize of 19622 bytes. It also drops winback.reg and winback.vbs (these are just initiator files). The end of the mirc.ini is modified to call the cat-penis.ini file. When initializing, it displays "Loading video using default browser, please wait..." and checks for presence of the file "C:\winback.vbs," if it does not exist, an Internet connection is started and tries to download a file called fucking.mpg. Irc connections are initialized using standard 6667. A visible text titled "[BatWorm 6 by Fyle]" and "Backdoor HTTPd by Fyle" may be seen. It may listen on socket httpd 4000. A private message to #fyle with victim's machinename/ip can be sent when connected. Listening is done using port 3995. Attempts can now be made to connect remotely to the victim's PC.

PWSteal.Bancos.B: This is a Trojan Horse that mimics the online interfaces of certain Brazilian banks in an attempt to steal account information. It is a minor variant of PWSteal.Bancos. This Trojan may arrive as an e-mail attachment called "book1.exe."

Stealthier: This Trojan has been found to be widespread among several universities. In these cases, the recent DCOM RPC vulnerability has been exploited to copy a backdoor Trojan and the patch for the DCOM RPC vulnerability. Exploited systems are patched, the backdoor is installed, and the Stealthier Trojan conceals both the backdoor and itself. The stealthier Trojan is designed to hide running processes, files, and registry keys. When run, any file name matching CSRS*.EXE will be hidden from the user. Details of the recent attack are as follows. Compromised systems contain the following files:

- %WinDir%\system32\csrsv.exe Stealthier trojan
- %WinDir%\system32\csrsu.exe ExeStealth packed BackDoor-TC trojan
- C:\update.exe MS03-026 patch

The following registry keys are present:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CSRSPX
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CSRSWIN1
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\CSRSPX
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\CSRSWIN1
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\CSRSPX
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\CSRSWIN1

The CSRSPX key is responsible for loading the Stealthier Trojan, to conceal the presence of any file named CSRS*.EXE (in this case the backdoor Trojan, as well as the Stealthier Trojan). Reports have varied in which TCP Port the backdoor Trojan is listening on, and is likely configured by the malicious user(s) responsible for these attacks.

Tr/Delf.r: Like other Trojans, Tr/Delf.r would potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following files:

- C:\Htv.exe (16.288 bytes)
- C:\Windows\System\Wininfo.exe (16.288 bytes)

So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
",main drive Loader"="wininfo.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
",main drive Loader"="wininfo.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
",main drive Loader"="wininfo.exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
",main drive Loader"="wininfo.exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
",main drive Loader"="wininfo.exe"

Troj/Autoroot-A (Alias: Exploit.Win32.Autorooter): Troj/Autoroot-A attempts to exploit a security vulnerability in Microsoft's DCOM RPC interface to invoke the backdoor Trojan Troj/IRCBot-G and allow unauthorized remote access to the compromised computer. Microsoft has issued a patch for the vulnerability exploited by this Trojan. The patch is available at:
<http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>.

Troj/QQPass-A: This is a password stealing Trojan.

Trojan.OptixKiller (Aliases: Backdoor.Optix, OptixKiller, Trojan.Win32.OptixKill.30): This is a Trojan Horse that attempts to terminate security software processes, such as antivirus programs and desktop firewall applications. This program is often distributed in conjunction with other malicious programs, like Backdoor.Optix.

Trojan.Progent (Alias: Trojan.Spy.ProAgent.121): This is a Trojan Horse that attempts to steal sensitive information and send it to the creator of the Trojan.

Woodcot: This Trojan consists of two binary PE files, ezones.exe 12320 bytes and wcot.exe 52625 bytes. The two files can be used to scan for vulnerable systems and connect to them. It scans an IP range for WEBDAV vulnerable Microsoft IIS 5.0 servers and tries to connect to found vulnerable systems. By default port 53 is used but a different port can be specified.